Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Protecting Consumers from SIM Swap and Port-Out Fraud	)	WC Docket No. 21-341
	)	
	)	

COMMENTS OF AT&T

Amanda E. Potter
Robert Vitanza
David Chorzempa
David Lawson

AT&T SERVICES, INC.
1120 20th Street, NW
Washington, DC 20036

Its Attorneys

November 15, 2021

TABLE OF CONTENTS

INTRODUCTION AND SUMMARY 1

DISCUSSION 3

I. AT&T COMBATS SIM- AND PORT-RELATED FRAUD USING A VARIETY OF INNOVATIVE, EVOLVING, AND EFFECTIVE TOOLS 3

A. AT&T Employs a Range of Tools As Needed to Deter Fraudulent SIM Swaps and Port-Outs. 4

B. AT&T's Practices Have Proven Highly Effective in Identifying and Limiting SIM- and Port-Related Fraud. 7

II. THE COMMISSION SHOULD ADDRESS SIM- AND PORT-RELATED FRAUD THROUGH A CONSENSUS-BASED APPROACH THAT LEVERAGES EXISTING EXPERTISE AND RESOURCES FROM INDUSTRY, THE COMMISSION, AND BEYOND 8

III. THE COMMISSION SHOULD PRESERVE CARRIERS' FLEXIBILITY TO DEVELOP AND EVOLVE EFFECTIVE TOOLS FOR COMBATING SIM- AND PORT-RELATED FRAUD 10

IV. THE COMMISSION SHOULD ESCHEW RULES THAT COULD UNDERMINE COUNTERMEASURES AND UNNECESSARILY INCREASE CUSTOMER FRICTION 12

CONCLUSION 18

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Protecting Consumers from SIM Swap and Port-Out Fraud	)	WC Docket No. 21-341
	)	
	)	

COMMENTS OF AT&T

AT&T Services, Inc.[1] ("AT&T") hereby submits these comments in response to the Federal Communications Commission's ("Commission's") Notice of Proposed Rulemaking ("NPRM") seeking comment on proposed amendments to its rules to reduce the potential for fraud in connection with subscriber identity module ("SIM") swap and port-out transactions.[2]

INTRODUCTION AND SUMMARY

We applaud the Commission's efforts to address this important consumer issue. AT&T is committed to protecting its customers and deterring bad actors intent on misusing processes designed for consumer benefit to inflict harm. SIM swaps allow customers to replace a defective SIM or, more commonly, to upgrade or replace an outdated, lost, stolen, or damaged phone, tablet, or other mobile device, without disruption to their wireless service. Meanwhile, port-outs allow customers to retain their telephone number when they change service providers. SIM swaps and port-outs are, in short, integral features of the competitive wireless marketplace. As such, AT&T devotes considerable effort and resources to ensuring that these processes function as they should, to the benefit of its customers. And as a general matter, they do – AT&T

[1] AT&T Services, Inc. is filing these comments on behalf of AT&T Mobility and its wireline operating affiliates.

[2] *Protecting Consumers from SIM Swap and Port-Out Fraud*, WC Docket No. 21-341, Notice of Proposed Rulemaking, FCC 21-102 (rel. Sept. 30, 2021) ("NPRM").

successfully and routinely processes hundreds of thousands of legitimate SIM swaps and port-outs without incident each month.

Motivated bad actors seek to abuse these mechanisms, with one goal: perpetrating theft, embarrassment, or other damage on the consumer being targeted. And the SIM swap or port-out is only a small part of the scheme to harm the consumer, as these incidents implicate a range of stakeholders not controlled by carriers (e.g., financial institutions, cryptocurrency companies, text message aggregators) that all play a role in the verification of customer identity. For its part, AT&T utilizes a variety of measures aimed at staying ahead of the culprits. As a result, we have successfully limited number-related fraud to a mere fraction of one percent of total SIM swaps and port-outs. While these scams are rare, AT&T fully recognizes the potential consequences for consumers when they occur. We welcome the opportunity to partner with the Commission and other stakeholders to target these fraud schemes and identify ways to provide additional protection to consumers.

Wireless carriers have developed substantial expertise in detecting and combating new forms of fraud. Significantly, AT&T has limited the incidences of fraudulent SIM swaps and port-outs by remaining flexible and varied in the tools it employs, allowing us to be at least as agile as the fraudsters. Thus, it is critical that the Commission preserve carriers' ability to use these capabilities and avoid applying rigid, one-size-fits-all restrictions that, depending on the circumstances, may be impractical and less effective at protecting consumers. The best way to combat ever-evolving fraud tactics is to allow industry players the ability to adapt and respond to these changing threats in real-time.

Accordingly, the Commission should defer any effort to adopt prescriptive rules such as waiting periods, mandatory notifications, and other requirements. Across-the-board prescriptive

rules would increase consumer frustration in nearly all SIM- or port-related transactions without a concomitant reduction in the risk, as over 99 percent of them are already legitimate. Instead, AT&T recommends the Commission first leverage existing resources and expertise – such as the Communications Security Reliability and Interoperability Council ("CSRIC"), the North American Numbering Council ("NANC"), the Technical Advisory Committee ("TAC"), or another appropriate body – before deciding on a course of action. Bringing together various stakeholders from the broader ecosystem will allow for a better understanding of how SIM swap and port-out scams operate, how the wireless industry is already combatting them, and how all stakeholders can reduce the risk of such fraud. Nevertheless, if the Commission's consideration of the record weighs in favor of a regulatory regime, any rules should be narrowly tailored to address the scope of risk and structured to avoid technical violations as carriers diligently act to protect their customers.

DISCUSSION

I. AT&T COMBATS SIM- AND PORT-RELATED FRAUD USING A VARIETY OF INNOVATIVE, EVOLVING, AND EFFECTIVE TOOLS

The NPRM seeks to "foreclos[e] the opportunistic ways in which bad actors take over consumers' cell phone accounts" and "proactively address[] the risk of follow-on attacks using stolen data."[3] AT&T wholeheartedly supports this objective but cautions that achieving it will require engagement by stakeholders that extend well beyond the wireless industry. That broader ecosystem includes banks, cryptocurrency companies, text aggregators, other financial institutions, and other platforms that over time, and with consumer cooperation, have come to rely on consumers' presumed possession of their wireless telephone number as a primary method

[3] NPRM ¶ 3.

– and sometimes sole method – of consumer identity verification. Depending on the particular circumstances, that may not provide adequate security.

The use of insecure methods of identity verification is an invitation to fraudsters to target consumers' wireless accounts, which they can then use to co-opt that verification mechanism in hopes of profiting off of, embarrassing, or otherwise causing harm to, the targeted consumer. Fraudsters typically will identify the specific consumer as their target well in advance, will gather information about the target from sources other than the consumer's wireless carrier (and sometimes from the target), and often will obtain control or access to the consumer's email account. If the bad actor is successful in taking over the target's wireless account, the fraudster then locates and gains access to the consumer's financial, social media, or other account for their nefarious purpose. The wireless carrier is but one link in a chain of steps contemplated by a highly motivated bad actor.[4] In reality, unless and until the other links in the chain are sufficiently secure, fraudulent attempts at SIM swaps and port-outs inevitably will persist.

A. AT&T Employs a Range of Tools As Needed to Deter Fraudulent SIM Swaps and Port-Outs.

The NPRM acknowledges that the wireless industry already is taking steps designed to prevent SIM and port-out scams and provides some examples of those efforts.[5] AT&T employs a diverse set of measures to help thwart these bad actors – above and beyond existing regulatory requirements and those proposed in the NPRM. AT&T therefore welcomes the opportunity to help compile a robust record regarding relevant legal and policy considerations before the Commission makes final decisions in this proceeding.

[4] From the wireless customer's and their provider's perspectives, these transactions in isolation amount only to a transfer of wireless service—from one device to another in the case of a SIM swap and from one provider to another in the case of a port-out.

[5] NPRM ¶¶ 50, 53.

As a threshold matter, wireless carriers possess strong incentives to prevent criminal schemes of all kinds – indeed, earning customers' trust by protecting their services and their data is a key basis on which carriers compete. To that end, AT&T has developed a range of tools that it employs to protect customers against fraudulent SIM swaps and port-out attempts, while still permitting legitimate transactions to proceed without undue delay. Significantly, these tools are tailored to different customers, services, and technologies because they must be. Just as there is no one-size-fits-all wireless service or technology to meet all consumer needs, there is no one-size-fits-all solution to deter bad actors from using a consumer's service or technology choice to advance their aims. A brief, non-exhaustive overview of AT&T's measures is set forth below.

Anti-fraud measures developed consistent with the Commission's existing authentication requirements protect consumers in most instances. For example, requiring customers to establish and then recite a pre-established password or PIN (for interactions occurring over the telephone or online) and conducting a review and comparison of a government-issued identification ("ID") (for interactions that occur in retail locations) typically are sufficient to ensure that the person attempting to engage in a transaction involving a particular account is authorized to do so. But no method of authentication is foolproof or effective in every instance. Customers forget passwords and lose their IDs (often at the same time they lose their wireless device). By the same token, passwords can be socially engineered, hacked or stolen, and driver's licenses and other government-issued ID cards can be faked. AT&T's various tools are designed to address these vulnerabilities.

Technology- and Analytics-Based Tools. AT&T relies on a diverse set of dynamic and evolving techniques to inform its approaches to customer authentication, just as other relevant players do. Indeed, retail employees in many situations no longer simply review a government-

issued ID presented by the customer. Instead, they may scan the customer's ID using technology that looks for indications of authenticity (or lack thereof). AT&T has leveraged data analytics to develop a sophisticated risk-scoring model for certain postpaid transactions. The model assigns a real-time transaction-specific risk score to certain transactions requested by a customer, including SIM changes and port-outs. The assigned score may trigger heightened authentication requirements or additional fraud prevention and mitigation techniques, such as those discussed below, prior to allowing completion of the requested transaction.

Transaction-Specific Notifications and Confirmations. For transactions meeting a specific threshold in the risk model, AT&T may use one or more forms of notification and related measures. At one threshold, AT&T sends no-charge SMS notifications – one-way communications sent to alert postpaid customers that their number was involved in a potentially unauthorized SIM swap or port-out transaction. Such notifications do not stop the transaction, but they alert customers that a potentially unauthorized SIM swap or port-out has been completed. At a higher risk threshold, AT&T uses SMS confirmations – two-way, no-charge communications sent to postpaid customers asking them to approve or reject a pending SIM swap or port-out transaction.

One-Time PINs. Independent of risk-based notifications and confirmations, AT&T routinely uses a one-time PIN delivered via SMS message or an outbound voice call to a postpaid customer's device for enhanced customer validation, including with SIM swaps. As referenced in the NPRM, AT&T has also implemented a Number Transfer PIN process to validate postpaid port-out transactions.[6] Customers must request the AT&T-provided PIN prior

[6] Verizon has adopted a similar port-specific PIN process. Any Commission rules adopted to protect against fraudulent port-outs must be flexible enough to allow carriers to continue using

to a port-out and provide that limited-life PIN to their new carrier, which submits the PIN with the port-out request for validation.[7]

Customer Outreach and Education. AT&T also engages in customer education to enhance their understanding of these issues. For instance, AT&T's website provides information about SIM swap scams and misuse of the porting process and offers guidance about how customers can protect themselves against such fraud.[8]

Continuous Innovation and Refinement. AT&T's suite of tools is not static. AT&T continually assesses the effectiveness of its countermeasures and refines them over time as needed. AT&T conducts routine forensic analysis of unauthorized SIM swaps and port-outs to assess the root cause and evaluate whether new or different countermeasures are appropriate to enhance security. This assessment has resulted in process changes, implementation of new security procedures, and more to guard against threats.

B. AT&T's Practices Have Proven Highly Effective in Identifying and Limiting SIM- and Port-Related Fraud.

AT&T's various complementary practices have proven to be highly effective at minimizing the number of successful SIM swap and port-out scams, confining these incidents to corner cases while also avoiding unnecessary burdens on customers. Of the hundreds of thousands of SIM swaps and port-outs that AT&T processes each month, only a fraction are

---

these types of temporary transaction-specific PINs assigned by the carrier, which offer superior protection as compared to permanent account-level passcodes assigned by customers.

[7] NPRM ¶ 53. AT&T cooperates with other carriers as needed to protect customers in porting transactions and to maintain the overall integrity of the port-out process. AT&T also works with law enforcement as necessary in order to identify bad actors.

[8] *See, e.g.*, AT&T, *What You Need to Know About SIM Swap Scams*, https://about.att.com/pages/cyberaware/ni/blog/sim_swap; AT&T, Cyber Aware, *Prevent Porting to Protect Your Identity*, https://about.att.com/pages/cyber-aware/news-information/blog/prevent_porting.html.

deemed fraudulent. By AT&T's calculation, more than 99 percent of the total SIM changes and port-outs it processes are legitimate. Far from posing a large or increasing threat, fraudulent SIM swaps and port-outs comprise an exceedingly small number of all such transactions processed.

Nevertheless, AT&T is not content with this success. Even a small number of incidents is material to the targeted customer. Moreover, bad actors have proven that they will not be deterred and will continue to try to exploit existing countermeasures. AT&T thus remains diligent in evolving its methods for rooting out and discouraging fraud.

As noted, SIM swap and port-out scams implicate third parties outside the Commission's jurisdiction. Accordingly, the Commission – through no fault of its own – cannot unilaterally end SIM swap and port-out scams by regulatory fiat. In this sense, the NPRM's conclusion that its customer proprietary network information ("CPNI") and local number portability rules are not "adequately protecting consumers against SIM swapping and port-out fraud" is not a fair indictment, as it implies that those rules are the primary source of such protection.[9] Realistically, these rules alone cannot solve the problem of SIM- and port-related fraud. What is needed is a team effort by all of the stakeholders discussed above.

II. THE COMMISSION SHOULD ADDRESS SIM- AND PORT-RELATED FRAUD THROUGH A CONSENSUS-BASED APPROACH THAT LEVERAGES EXISTING EXPERTISE AND RESOURCES FROM INDUSTRY, THE COMMISSION, AND BEYOND

The most effective mitigation of SIM- and port-related fraud will require greater collaboration and education of stakeholders across the ecosystem. The NPRM is relatively silent as to critical roles played by other relevant participants outside the communications sector. Thus, the Commission can and should seek broader and deeper stakeholder engagement as a

[9] NPRM ¶ 3.

more constructive and critical first step in this proceeding. Existing vehicles at the Commission's disposal offer a ready-made forum for that to occur. AT&T encourages the Commission to address the problem of SIM swap and port-out scams through these avenues before it considers adopting or amending any rules.

Several mechanisms within the Commission's purview are well-suited to consider the issue of SIM swap and port-out scams and recommend actions to deter them. For instance, the Commission could convene stakeholders through a CSRIC or NANC working group or expand the focus of the TAC's Mobile Device Theft Prevention Working Group to encompass the threat posed by SIM- and port-related fraud. These forums are organized to address broader challenges that, like SIM swap and port-out scams, implicate diverse stakeholders in different industry segments (including those outside of the Commission's traditional jurisdictional reach), are constantly changing, and are amenable to being addressed through voluntary best practices. Any of these options would offer a structured setting for the Commission and industry to jointly pursue the flexible, outcomes-based approach demanded by the occurrence of fraudulent SIM swaps and port-outs.

This approach would align with broader federal efforts under the current Administration to partner with industry to enhance security and combat malicious actors, such as the ongoing work of the Cybersecurity & Infrastructure Security Agency ("CISA") under the auspices of the Department of Homeland Security. The Commission itself is already forging a collaboration with CISA through their joint leadership of CSRIC VIII, and that model would serve the Commission's goals in this proceeding as well. Given CISA's core mission to manage risks to critical infrastructure and focus on addressing risks posed by interdependencies between critical infrastructure sectors like the communications and financial sectors (which otherwise do not

share common oversight), that agency may be in a prime position to draw all necessary stakeholders to the table. And CSRIC – with its respected track record and deep expertise in communications security – may provide a uniquely suitable forum for these discussions. AT&T and other wireless carriers are presently involved in these groups, and AT&T stands ready to work with the Commission more closely and constructively to combat number-related fraud.

III. THE COMMISSION SHOULD PRESERVE CARRIERS' FLEXIBILITY TO DEVELOP AND EVOLVE EFFECTIVE TOOLS FOR COMBATING SIM- AND PORT-RELATED FRAUD

A prescriptive approach, such as that reflected in some of the NPRM's proposals, would introduce rigidity where flexibility is needed. As the NPRM reminds, the Commission long ago concluded in the CPNI context that "techniques for fraud vary and tend to become more sophisticated over time," such that carriers "need leeway to engage emerging threats."[10] But the need for carrier flexibility warrants even more emphasis than the NPRM gives it. Carriers must remain agile and have sufficient latitude to employ and refine their practices to effectively combat SIM swap and port-out fraud.

Fundamentally, SIM swap scams and port-out fraud occur in a constantly shifting threat environment. Bad actors perpetually look for creative ways to gain access to consumers' financial or social media accounts by leveraging an assortment of tools, technologies, or techniques. In turn, carriers combat such malicious activity by leveraging ever-evolving tools, technologies, and techniques of their own, all while avoiding unreasonable burdens on legitimate customers. Bad actors pivot in response, which triggers additional carrier innovation and

[10] NPRM ¶ 27 (quoting *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, CC Docket No. 96-115, WC Docket No. 04-36, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 ¶ 3 (2007)). *See also id.* ¶¶ 27, 28, 55.

response. And so on. In this cyclical environment, no tools or methods will prevent all SIM swap scams or port-out fraud. But we can mitigate the impact by keeping its overall incidence low and quickly responding when an incident occurs. Effective mitigation requires an agile approach to managing these risks that can only be achieved within a flexible framework.

For example, passwords – the touchstone for customer authentication since the Commission's 2007 CPNI Order – can be susceptible to social engineering and other forms of attack. While passwords remain a useful and typically effective authentication tool, especially when used in combination with other security mechanisms, that may not be the case in the future. New forms of network-based authentication offer promise for preventing unauthorized access incidents in ways that may be more user-friendly as well. In addition, while government-issued IDs typically are sufficient for in-person verification, professional fraudsters can take advantage of well-produced fake IDs. Thus, carriers must be agile and innovative in fighting fraud and should not be anchored by prescriptive requirements tied to specific technologies or methods.

Customer needs also vary. AT&T provides customers a range of products and services to meet different wireless communications needs. The diverse characteristics of these customers and the products and services they utilize lend themselves to different risk-management approaches. While most customers desire ready, on-demand access to their accounts for plan changes, device upgrades, and the like, other customers who would be high-value targets for bad actors may desire heightened security measures to prevent unauthorized access to their accounts. Such targeted customers may have a lower risk tolerance for fraud and a greater tolerance for high-friction measures that hinder their ability to easily or quickly swap SIMs or to port-out numbers. Any regime the Commission might seek to put in place must account for the full range of needs and preferences of the consumers ostensibly being protected.

Similarly, the threat of SIM swap or port-out fraud is not equivalent in all circumstances, rendering prescriptive one-size-fits-all requirements merely a nuisance to most consumers. For example, a data-only service, particularly one in which the SIM or telephone number is not SMS- or voice-enabled, should not be subject to the same rules as a wireless service tied to a consumer's handset. Moreover, many businesses have the need to engage in bulk SIM swaps when upgrading equipment and need a solution to accommodate the bulk process that goes beyond the Commission's existing business customer exception. Nevertheless, wireless providers have effective means of authenticating such customers and therefore should not be required to ensure a number-by-number authentication process.

In light of these numerous variables, carriers should be permitted to continue to employ risk-based and customer-focused approaches to SIM swaps and port-outs that account for differing levels of risk, a fluid technological and threat landscape, and diverse customer needs. Again, existing forums such as CSRIC and the TAC are ideally suited to host further development of that type of framework.

IV. THE COMMISSION SHOULD ESCHEW RULES THAT COULD UNDERMINE COUNTERMEASURES AND UNNECESSARILY INCREASE CUSTOMER FRICTION

Prescribing specific methods wireless carriers must employ to combat fraudulent SIM swaps and port-outs would greatly restrict their flexibility to update practices and tailor them to support the wide array of needs for diverse types of customers and services. If anything, specific mandates in this context could provide a roadmap for bad actors who would quickly tailor their tactics to circumvent them, while restricting consumer choice and imposing delays and other burdens upon the overwhelming majority (more than 99 percent) of transactions that are perfectly legitimate. Even proposals that have merit in *certain* circumstances should not be

foisted onto all carriers in *all* circumstances. Rather, at most they should remain tools in the toolbox that carriers have the flexibility to implement at their discretion.

Below, AT&T addresses certain proposals and inquiries in the NPRM that would be particularly problematic if adopted.

1. Fixed authentication methods

The NPRM would require carriers to use "a secure method of authenticating its customer" before effectuating a SIM swap and then lists four methods that would satisfy that standard.[11] Although the specified authentication methods are "familiar ones, already used by consumers and companies[,]"[12] they would introduce new and often unwanted complexities in the SIM swap process for carriers and their customers.

Fundamentally, requiring the use of particular authentication methods for every SIM swap would impose tremendous burdens on carriers and customers without clear additional benefit. Carriers are already authenticating customers using one or more of the methods identified in the Commission's existing and/or proposed rules. Customers must show their government-issued ID at retail, provide their account passcode to call center representatives, and input their username and password online. The proposed rules would add another authentication step to complete a routine transaction, such as an upgrade, but that proposed step may not be the best way to perform this second factor of authentication.

Those additional authentication steps also may be wholly unnecessary for some transactions. As discussed, AT&T employs data-driven analytics to make an initial risk assessment for specific postpaid transactions, which drives confidence in the authenticity of the

[11] NPRM ¶ 22 & App. A, § 64.2010(e).

[12] NPRM ¶ 25.

transactions and allows them to be completed without delay or burden to the customer. The NPRM would eliminate a carrier's discretion to utilize such customer-friendly approaches to customer authentication by effectively requiring additional authentication measures even when the carrier's processes have already served that purpose.

Moreover, locking in a particular list of authentication methods would play into bad actors' hands by discouraging carriers from adopting new methods not expressly blessed by the Commission's rule, while inhibiting the ability of carriers and other stakeholders to innovate, as necessary and appropriate, to address evolving threats. The practical effect of the list is that carriers will feel constrained in using non-listed methods for fear that anything else would be unauthorized.[13] Indeed, carriers, courts, and consumers reasonably could conclude that password- and PIN-based authentication methods are the only acceptable authentication methods for SIM changes contemplated under the Commission's rules.

Lastly, as the Commission has contemplated, fixed authentication methods for SIM changes and port-outs will provide a roadmap to bad actors.[14] It is an unfortunate reality that the more documented and public the processes, the less effective they will be at protecting consumers from number-related fraud. The Commission should endorse a flexible standard that

[13] While the NPRM states that the listed methods "shall not be exhaustive," it then provides that any "alternative customer authentication measure" must be "a secure method of authentication" – a vague standard that begs the question of what other methods the Commission would consider to be "secure," and in turn would likely force carriers to revert to the enumerated measures. Further, the proposed rule lacks the sort of language that makes clear a list is merely exemplary rather than exclusive. *See, e.g.*, *Petition of the United States Satellite Broadcasting Company,* 1 FCC Rcd 977, 978 (1986) (stating that when the Commission listed potential uses and included "and the like" after the list, it did not intend to make the list exclusive); *Masters Pharm., Inc. v. DEA*, 861 F.3d 206, 221 (D.C. Cir. 2017) ("[It is] well established that the word 'include' often precedes a list of 'illustrative' examples, rather than an exclusive list ….").

[14] NPRM ¶¶ 27, 55.

carriers authenticate customers prior to effectuating a SIM change, while enabling them to decide how that occurs and to continue innovating and responding rapidly to immediate threats.[15]

2. Customer notifications

Customer notification is already a key component of AT&T's efforts to deter SIM swap and port-out fraud. As discussed above, AT&T relies on different forms and timing of notices tailored to the likelihood that a transaction is fraudulent. But the NPRM's proposal of an across-the-board notification requirement for all SIM swaps and port-outs does not allow for such a tailored approach.[16]

First, the proposed rules would mandate notice even where it is not necessary.[17] As discussed, AT&T employs various tools to assess the risk level of a particular postpaid SIM change or port-out request and very often can determine at the outset that a request is legitimate – in which case, no notice confirming its legitimacy should be necessary. In that circumstance, such a gratuitous notice would frustrate legitimate customers whose transactions do not justify scrutiny while imposing burdens (not to mention risks of technical rule violations) on the carrier for no discernible purpose. And notices would occur so frequently that customers would eventually become numb or immune to them or tire of and consciously choose to ignore them, thus undermining all value they might otherwise have when the threat of fraud is real.

---

[15] Proposed rule § 52.37(a)-(c), addressing data fields to validate a port-out, should retain the flexibility to allow carriers to continue using temporary transaction-specific PINs assigned by the carrier *in lieu of* account-level passcodes assigned by customers, as the temporary PIN offers superior protection.

[16] NPRM ¶¶ 34-36.

[17] NPRM, App. A, § 52.37(d) ("A wireless provider . . . *shall notify* an end user customer . . . . *before* executing a simple wireless-to-wireless port request."), §64.2010(h) ("Telecommunications carriers *shall notify* customers immediately of any requests for SIM changes . . . .") (emphases added).

Further, the proposed rules as written (i.e., "shall notify") could be read to require notification before the transaction completes, even where such notification is not feasible. As worded, this would impose a strict liability standard that is the antithesis of the flexible framework required in this context or, at best, inject the potential for unnecessary delay into the port-out process. Carriers can attempt to notify a customer before completing a port-out, but they cannot guarantee actual notification to the customer will occur. Notification may fail or be delayed if a notice sent to the customer goes unread (e.g., the customer has turned-off their device or placed it in silent mode), is delayed, or does not reach its destination (e.g., the customer is outside a coverage area or using a third-party Wi-Fi network). Even if across-the-board notice is the goal, which it should not be, a carrier's obligation should be limited to sending notice, not guaranteeing its delivery or receipt before completion of the transaction.

Meanwhile, the proposed rule requires that the notice of a port-out request *must* occur by text message to the primary account telephone number or by push notification.[18] Though these modes of communicating with customers may currently be the least fallible, that may not always be the case. Other means of communicating with customers are likely to arise as technology evolves. Also, customers whose devices are lost, stolen, or damaged can still have their number ported, but they would not receive an SMS or push notification. For these reasons, the Commission should not mandate the specific method carriers use to send notices to or otherwise communicate with their customers. Instead, carriers should be permitted to communicate with their customers via the means they deem to be most effective in a particular context.

[18] NPRM, App. A, § 52.37(d) ("A wireless provider shall provide this notification . . . via text message . . . or via push notification.").

3. Account freezes

The NPRM seeks comment on whether to require wireless carriers to offer customers the option to freeze (i.e., lock) their accounts.[19] Account locks can be an effective tool to increase the security of customer accounts on occasion, but they are not needed to manage the risk of fraud in every case and for every customer. Further, building a system that is capable of widespread adoption of this measure would entail significant carrier costs and time for questionable gain.

Moreover, the utility of an account lock feature varies by service. Prepaid service, for example, is not amenable to this measure. Some prepaid customers provide little personal information when they activate their account. If those customers lock their account and their device is later lost, broken, or stolen, they would be unable to provide their wireless carrier with authentication information sufficient to unlock the account. Thus, an account lock would likely create more of a burden than a benefit for prepaid customers and their carriers. Even for postpaid accounts, an account lock can be a source of friction when the customer forgets having placed the freeze on the account or dislikes the efforts needed to unfreeze the account. Thus, an account freeze option should remain a tool that carriers can choose, but are not required, to offer.

4. 24-hour waiting period

The NPRM asks if delaying SIM swaps for 24 hours after notice would effectively protect customers from fraudulent SIM swaps.[20] It would not – in fact, it would likely frustrate them, for a number of reasons. First, as discussed above, even a delay after notice would not eliminate all fraudulent SIM swaps. Second, a 24-hour waiting period would not be workable

[19] NPRM ¶ 39.

[20] NPRM ¶ 37.

for the vast majority of consumers. As the Commission recognizes, cell phones "are an essential part of everyday life" for consumers.[21] In light of that reality, forcing a customer with a lost, stolen, or damaged phone to wait 24 hours (or just a few hours for that matter) before obtaining an active replacement would at best frustrate the consumer (who would likely but incorrectly fault the carrier for the delay), and, at worst, threaten the customer's safety and impair her ability to engage in commerce, work, and education. Last, this burden of a 24-hour waiting period, which would be imposed on all customers, far outweighs the benefit of avoiding a relatively small number of fraudulent SIM swaps.[22]

5. Two employee sign-off

Similarly, requiring two employees to sign off on every SIM change would also unjustifiably, and significantly, burden the more than 99 percent of legitimate SIM swaps.[23] Such a step would be time-intensive, increasing the length of the SIM swap process, and would remain susceptible to social engineering and collusion. Also, it is unclear how the second employee would evaluate the transaction separately from the first employee, or what would happen if, as can occur, a second employee is not available. Last, the frequency (and thus sheer number) of legitimate SIM changes makes this suggestion infeasible in practice.

CONCLUSION

For these reasons, AT&T encourages the Commission to leverage its own and industry expertise and resources to bring *all* relevant stakeholders together to address the threat of fraudulent SIM swaps and port-out requests, while avoiding prescriptive regulations that would

[21] NPRM ¶ 1.

[22] Delays in the porting-out process are inadvisable for similar reasons and because they would discourage ports, to the detriment of consumer choice and marketplace competition.

[23] NPRM ¶ 38.

constrain carriers' flexibility. AT&T remains eager to work with the Commission and all other stakeholders to refine best practices in this context.

November 15, 2021

Respectfully submitted,

/s/ Amanda E. Potter

Amanda E. Potter
Robert Vitanza
David Chorzempa
David Lawson

AT&T SERVICES, INC.
1120 20th Street, NW
Washington, DC 20036

Its Attorneys